# A Fuzzy Security Investment Decision Support Model for Highly Distributed Systems

Emrah Yaşasın, Gerhard Rauchecker, Julian Prester, Guido Schryen
Department of Management Information Systems, Universität Regensburg
{emrah.yasasin, gerhard.rauchecker, guido.schryen}@wiwi.uni-regensburg.de
julian.prester@stud.uni-regensburg.de

***Abstract*—The economic aspect of information security is a comparatively new discipline so that there is hardly any extensive research work. This applies in particular to measures in highly distributed systems which have been neglected in previous research. The present paper focuses on the security investments in such systems. We augment an existing research about a fuzzy decision support model by defining appropriate operators in order to applicate this work in practice. The proposed model includes uncertainty with respect to the impact of investments on the achieved security levels of components of the distributed system. We further develop a heuristic to solve the problem and test the heuristic experimentally. The paper concludes with a discussion and gives an outlook to future work in the context of security investments.**

***Keywords*-fuzzy security investments; decision support model; highly distributed systems; fuzzy optimization; monte carlo heuristic;**

## I. Introduction

The economic view of security measures has moved more back into focus of the IT security research in almost every communication-based field of application. However, the economic aspect of information security is a comparatively new discipline so that there is hardly any extensive research work neither in terms of planning ("ex ante" view) nor in evaluation ("ex post" view) of IT security measures [1]. In the context of highly distributed information and communication systems, the importance and the complexity of economic security research work is gaining in significance. The growing importance and thus the direct economic value results from the fact that technologies like RFID or concepts like "cloud computing", "service oriented computing", "internet of things" and social networks affect the everyday life of many people. Further, there are much more resources to manage for the security of highly distributed systems compared with isolated systems [2].

The increase of complexity is primarily based on the factors of extension, dynamics and stakeholder: 1) Extension: IT security measures have to be managed across organizational borders and local technical infrastructures. 2) Dynamics: Due to the higher dynamics of highly distributed systems, planning and evaluation of IT security measures are cycles which are continuously getting shorter. 3) Stakeholder: Many stakeholders with various preferences and their security planning are involved in highly distributed systems. These factors are insufficiently addressed in previous research for the economic evaluation of IT security measures. Thus, there is no suitable economic planning and evaluation basis for the application in highly distributed systems existing. [3]

Arising from these shortcomings, the overarching objective is to answer the questions how the decision-making process for IT security measures can be provided (ex ante view). However, decision makers often face uncertainty concerning budget constraints, costs and security levels within highly distributed systems. Unfortunately, with the lack of large amounts of historical data, it is a hard task to quantify uncertainty with probabilities so that the application of probabilistic approaches is not conducive. We therefore draw on fuzzy set theory which is an established uncertainty theory in the absence of probabilities and in the presence of subjective assessments.

In this paper, we give an extension of [4] who proposes a generic IT security investment decision-making model based on fuzzy set theory. We adopt and derive operators and give a pseudocode of a Monte Carlo heuristic in order to make the generic model applicable in practice. In particular, the paper is organized as follows: the next section introduces related work. The third section outlines the application context followed by the used methodological approach. Subsequently, we propose operators and a Monte Carlo heuristic to solve the optimization model. This research article closes with a discussion of findings and an outline of next steps.

## II. Related Work

The literature on economic IT security research can be broadly divided into microeconomic and management oriented approaches. Whereas the microeconomic perspectives tend to focus on game theoretic analysis for IT security investments (cf. [5], [6]), the management oriented perspectives address issues related to decision support for IT security investments and their evaluation.

The questions to decision support are mainly dominated by financial cost/benefit analyses. On the one hand, bases of investment theory are adapted [7], notably "the return on security investment" (cf. [8], [9]), the "net present value model" [10], [11] and the usage of stochastic models to determine potential losses [12]. On the other hand, new security enforcing models are generated which determine the optimal investment amount in IT security measures from various security threat views [11], [13]. To a lesser extent, some approaches are based on

market mechanisms [14] and use insurances as an instrument for risk management [15] or derivatives [16] for instance.

However, there is no comprehensive method existing for decision support in IT security investments [17]. Furthermore, in the context of highly distributed information and communication systems, the existing approaches are suitable to only a limited extent:

1) Central available information resources and systems are concerned as security assets that are in the area of single organization units. This assumption is not given in service-oriented computing for instance.
2) Decision models assume that risk observations are based on historical data and probabilistic informations. However, these informations are often not available and turn out to be poorly suited for modeling of very unlikely events. Moreover, they do not consider individual risk preferences [18].
3) Investment decisions are based on pure financial evaluations and ignore that security measures should include non-financial objectives such as confidence in social networks or the availability of a critical infrastructure. The evaluation of IT security measures deals with their efficiency (economy and efficiency in resource utilization) and their effectiveness (quality) and constitutes therefore an essential point of the whole IT management. Central tasks are the collection, analysis and the reporting of data about the performance of IT security measures [19]. In the existing literature, there are only few investigations dealing with efficiency and effectiveness of IT security measures. The focus of these researches is on the generation and the application of metrics. A practice-oriented enumeration of metrics is found in [19], some texts address the influences of IT security measures on stock prices (cf. [20]) and in [21], the economic effects of a specific instrument are examined (role-based access control)). However, the literature does not provide a theoretical substructure for process models, data acquisition support and metrics for the evaluation of IT security measures.

Therefore, in the field of highly distributed information and communication systems, the following research shortcomings can be identified: First, as IT security investments in complex highly distributed areas are made across organizational boundaries, the identification and collection is a key concern of information acquisition. There are no findings which data are collected from which participant and which data should be available. Second, whereas the investments in IT security measures are the input for economic and effectiveness analysis, the question arises how the output can be measured. This requires an evaluation process, including metrics, how "distributed security" can be measured and for which data is available. Metrics, such as those that exist for software security [22], are not known yet.

We have argued that there is a need to facilitate decision making and to improve performance and accountability based on information security. However, as we are not only interested in measurement or the quantification of information, we go one step further and strive to apply and extend the proposed approach of [4] in order to analyze it in a highly distributed environment. Therefore, contrary to existent research, the paper aims to close the research gap and provides a methodological proper attempt to consider the ex ante view thoroughly.

## III. A Possible Scenario

Consider an enterprise which has various distributed systems, servers and applications. Assume that every computer, server and application has a certain security level and that the enterprise can only contribute a limited budget to increase these security levels. We can consider that the overall security of the highly distributed system is determined by the security of each component. The aim is to maximize the overall security while facing some constraints. The first one is about the budget: the enterprise provides on the one hand a certain budget for the overall security investment and on the other hand certain component budgets. The costs for increasing the security level is also closely related to the component's security level. In other words, for getting secure components more secure is more expensive than for lower secure components. Second, there might be least acceptable security levels for each component that have to be fulfilled.

The question therefore arises whether the overall security can be maximized while taking into account all components in the highly distributed system and the restrictions the enterprise is faced to. The next section provides the answer for this question. The decision support model maps all these facts into an optimization model which is described and solved in the next sections.

## IV. Decision Support Model

In order to support decisions in the area of security investments, we adopt a fuzzy decision support model formulated by Schryen [4]. To formulate our model, we first have to give elementary definitions of the fuzzy set theory that we are going to use in our approach.

*Definition 1:* Let $X$ be a crisp set. A fuzzy set $\widetilde{A}$ in $X$ is a set of ordered pairs

$$\widetilde{A} = \{(x, \mu_{\widetilde{A}}(x)) | x \in X\}$$

where $\mu_{\widetilde{A}} : X \to \mathbb{R}_{\geq 0}$ is called the membership function of $\widetilde{A}$ in $X$. The (crisp) set of elements that belong to the fuzzy set $\widetilde{A}$ at least to the degreee $\alpha$ is called the $\alpha$-cut $\widetilde{A}_\alpha = \{x \in X | \mu_{\widetilde{A}} \geq \alpha\}$. $\widetilde{A}$ is convex if all $\alpha$-cuts are convex.

*Definition 2:* A fuzzy number $\widetilde{A}$ is a convex fuzzy set $\widetilde{A}$ in $\mathbb{R}$ such that $\mu_{\widetilde{A}} : \mathbb{R} \to [0, 1]$ is piecewise continuous and there exists exactly one $x_0 \in \mathbb{R}$ with $\mu_{\widetilde{A}}(x_0) = 1$ ($x_0$ is called the mean value of $\widetilde{A}$). A triangular fuzzy number $(a/b/c)$ with $a < b < c \in \mathbb{R}$ is the fuzzy set $\widetilde{A}$ in $\mathbb{R}$ with the membership function

$$\mu_{\widetilde{A}}(x) = \begin{cases} \frac{1}{b-a} \cdot x - \frac{a}{b-a}, & \text{if } a \leq x \leq b \\ -\frac{1}{c-b} \cdot x + \frac{c}{c-b}, & \text{if } b \leq x \leq c \\ 0, & \text{else.} \end{cases}$$

*Definition 3 ([23]):* A linguistic variable is characterized by a quintuple $(x, T(x), U, G, \widetilde{M})$ in which $x$ is the name of the variable; $T(x)$ denotes the term set of $x$, that is, the set of names of linguistic values of $x$, with each value being a fuzzy variable denoted generically by $X$ and ranging over a universe of discourse $U$; $G$ is a syntactic rule (which usually has the form of a grammar) for generating the name, $X$, of values of $x$; and $M$ is a semantic rule for associating with each $X$ its meaning, $\widetilde{M}(X)$, which is a fuzzy subset of $U$. A particular $X$ - that is, a name generated by $G$ - is called a term.

With these definitions, we state our formulation of the decision support model. We assume that the security description of a distributed system, which consists in the set $A$ of components, is given by the propositional logical formula

$$(A_{11} \vee \ldots \vee A_{1n_1}) \wedge \ldots \wedge (A_{m1} \vee \ldots \vee A_{mn_m}) = \bigwedge_{i=1}^{m} \left( \bigvee_{j=1}^{n_i} A_{ij} \right)$$

and propose the following fuzzy decision support model.

$$\max \bigwedge_{i=1}^{m} \left( \bigvee_{j=1}^{n_i} X_{ij} \right) =: Z((X_{ij})_{ij}) \tag{1}$$

$$\text{s.t.} \quad X_{ij} \succ B^0_{ij}, \quad i,j|A_{ij} \in A \tag{2}$$

$$X_{ij} \succ B^*_{ij}, \quad i,j|A_{ij} \in A \tag{3}$$

$$\sum_{i,j|A_{ij} \in A} c_{ij}(X_{ij}, B^0_{ij}) \prec b \tag{4}$$

$$c_{ij}(X_{ij}, B^0_{ij}) \prec b_{ij}, \quad i,j|A_{ij} \in A \tag{5}$$

The constraints are crisp which means that they have to be fulfilled strictly. In order to solve this model, we have to explain how to operate with and compare fuzzy sets. This is presented in the next section. First, we want to explain the meaning of our objective function and constraints. The variables $X_{ij}$ are linguistic fuzzy variables which can for example indicate the security level of component $A_{ij}$ (e.g. "moderately secure" or "very secure"). In this context the goal of (1) is to maximize the overall security of $A$.

The numbers $B^0_{ij}$ respectively $B^*_{ij}$ are fuzzy numbers and denote the start security level respectively the least acceptable security level of component $A_{ij}$, see constraints (2) and (3). The parameters $b$ and $b_{ij}$ are fuzzy numbers which represent the total budget $b$ available for a security investment and the budget $b_{ij}$ available for investing into component $A_{ij}$. The values $c_{ij}(X_{ij}, B^0_{ij})$ are also fuzzy numbers which indicate the total cost to raise the security level of compenent $A_{ij}$ from $B^0_{ij}$ to $X_{ij}$. Consequently, constraints (4) and (5) model budget restrictions.

## V. Monte Carlo Heuristic

In order to apply the decision model in a practical context, we develop a Monte Carlo heuristic. For this, we need to develop several concepts, namely the ranking of fuzzy sets, the addition of fuzzy numbers and the logical AND and OR connection of fuzzy sets.

To sum up fuzzy numbers, we choose a definition which is based on $\alpha$-cuts and the fact that a fuzzy subset of $\mathbb{R}$ is uniquely defined by its family of $\alpha$-cuts.

*Definition 4:* Let $(S_1, \mu_1), (S_2, \mu_2)$ be two fuzzy numbers and $([a_1(\alpha), b_1(\alpha)])_{\alpha \in [0,1]}$ (resp. $([a_2(\alpha), b_2(\alpha)])_{\alpha \in [0,1]}$) be the family of $\alpha$-cuts of $S_1$ (resp. $S_2$). We define the $\alpha$-cuts of the fuzzy number $S_1 + S_2$ by $(S_1 + S_2)_\alpha := [a_1(\alpha) + a_2(\alpha), b_1(\alpha) + b_2(\alpha)]$ for all $\alpha \in [0,1]$.

For defining a ranking on fuzzy sets, we refer to [24], [25] who propose a ranking approach based on the center of gravity of fuzzy sets.

*Definition 5:* Let $(S, \mu)$ be a fuzzy set. The center of gravity is defined by

$$F(S) := \frac{\int_{\mathbb{R}} \mu(x) \cdot x \ \mathrm{d}x}{\int_{\mathbb{R}} \mu(x) \ \mathrm{d}x}$$

and induces a linear quasiorder on the class of fuzzy sets by setting

$$S_1 \prec S_2 :\Leftrightarrow F(S_1) \leq F(S_2)$$

for fuzzy sets $(S_1, \mu_1), (S_2, \mu_2)$.

*Definition 6:* Let $(S_1, \mu_1), (S_2, \mu_2)$ be fuzzy sets. We define the OR connection by

$$S_1 \vee S_2 := \max\{S_1, S_2\}$$

and the AND connection by

$$S_1 \wedge S_2 := \min\{S_1, S_2\}$$

where the min and max operators base on the ranking from definition 5.

Now we have the ability to formulate a Monte Carlo-based solution heuristic presented in the following. Let $\mathcal{T} = T(X_{ij})$ be the set of linguistic values which underlie the linguistic variables $(X_{ij}, T(X_{ij}), U, G, \widetilde{M})$.

1 Initialize $X^* := (\max\{B^0_{ij}, B^*_{ij}\})_{ij}$
2 Initialize the current best objective value $Z^* := Z(X^*)$
3 For each $(i,j)$ set $\mathcal{A}_{ij} := \Big\{ T \in \mathcal{T} | \widetilde{M}(T) \succ B^0_{ij}$ and $\widetilde{M}(T) \succ B^*_{ij}$ and $c_{ij}(\widetilde{M}(T), B^0_{ij}) \prec b_{ij} \Big\}$.
4 **for** $\tau = 1, \ldots, maxiter$ **do**
5  Choose $X_{ij} \in \mathcal{A}_{ij}$ randomly for each $(i,j)$
6  **if** $(X_{ij})_{ij}$ is infeasible **then continue**
7  **else**
8  **if** $Z((X_{ij})_{ij}) \prec Z^*$ **then continue**
9  **else**
10  Set $X^* := (X_{ij})_{ij}$ and $Z^* := Z(X^*)$
11  **endif**
12  **endif**
13 **endfor**
14 **return** $X^*$ and $Z^*$

The definition of $\mathcal{A}_{ij}$ is motivated by the constraints (2), (3) and (5) and aims at producing feasible random solutions (in

line 5) more likely than without this setting. Another advantage of this definition is that the feasibility test in line 6 of the algorithm is only about fulfilling constraint (4). We would like to mention that the concept of ranking fuzzy sets is essential in this algorithm.

## VI. Computational Experiments

### A. Data Generation

We adopted and slightly modified four different security levels from [4], namely *insecure*, *moderately secure*, *very secure* and *highly secure*. For the membership function of each security level we have chosen invers quartic functions, see Figure 1 below:

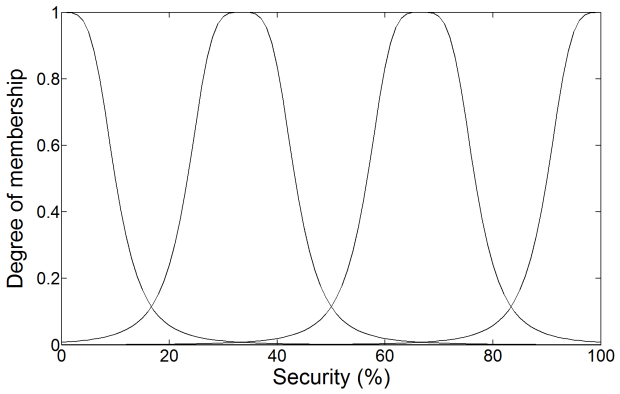


Fig. 1. Security levels and their membership functions.

We generated scenarios with different types of architectures $m = 1, \ldots, 10$ and security properties $n = 1, \ldots, 10$, which should cover the structure of highly distributed systems. For each problem size, we randomly generated 100 instances and solved all of them in our Monte Carlo simulation with 100 iterations. Finally, we averaged the $F$ values (see Definition 5) of the objective function $Z$.

The start security levels as well as the least security levels of each component were generated with the distribution presented in Table I.

TABLE I
START AND LEAST SECURITY LEVEL DISTRIBUTIONS

| | insecure | moderately secure | very secure | highly secure |
|---|---|---|---|---|
| $B^0_{ij} \sim$ | 30% | 60% | 5% | 5% |
| $B^*_{ij} \sim$ | 20% | 65% | 10% | 5% |

In the following, we will introduce the costs and budget constraints of our experiments. All costs and budgets are expressed as symmetric triangular fuzzy numbers $(0.9a/a/1.1a)$ with mean value $a \in \mathbb{R}$.

To upgrade the security from the start level $B^0_{ij}$ to a security level $X_{ij}$, we used the cost matrix illustrated in Table II.

As can be gathered from that table, there are six cost levels $d_1, \ldots, d_6$ for security upgrades. For each $i, j$, we randomly choose an index $k = k_{ij} \sim U(1, 6)$ by a discrete uniform distribution and set $\widetilde{b_{ij}} := d_k$ and $b_{ij} := \max\{\widetilde{b_{ij}}, c(B^*_{ij}, B^0_{ij})\}$ for each component. The reason for this is to enable the update to its required least security level.

TABLE II
UPGRADE COSTS

| $c_{ij}(X_{ij}, B^0_{ij})$ | insec. | mod. sec. | very sec. | highly sec. |
|---|---|---|---|---|
| insec. | 0 | 0.1 | 0.5 | 1 |
| mod. sec. | 0 | 0 | 0.4 | 0.9 |
| very sec. | 0 | 0 | 0 | 0.5 |
| highly sec. | 0 | 0 | 0 | 0 |

We proceed for the generation of the overall budget as follows: we applied our Monte Carlo heuristic to all generated instances for each problem size without the overall budget restriction and averaged the costs of upgrading to the solutions of the Monte Carlo heuristic for each problem size. After that, we use these averages as the overall budget constraint for each problem size.

### B. Results

To determine the explanatory (power of) factors that influence the security level value $F(Z)$, we perform a linear regression with $F$ as the dependent variable and $m$ and $n$ as the independent variables. The linear regression model provides a simple but useful decomposition of the security value into the components $F = \beta_0 + \beta_1 \cdot m + \beta_2 \cdot n$.

TABLE III
STATISTICS OF THE LINEAR REGRESSION.

| | Estimate | Pr(> \|t\|) |
|---|---|---|
| (Intercept) | 52.7189 | < 2e-16 |
| m | -0.9181 | 0.000331 |
| n | 5.0966 | < 2e-16 |
| Multiple R-squared | 0.8197 | |

The linear regression can be expressed as $F = 52.7189 - 0.9181 \cdot m + 5.0966 \cdot n$. The multiple $R^2$ shows a highly fit of 0.8197 so that we can state that our linear model explains 81.97% of all the variability of the response data around its mean. One can see that both independent variables $m$ and $n$ are statistically highly significant at the p-value $0.001$.

Figure 2 shows the achieved security levels of the randomly generated model instances for different types of architectures/security properties (combinations of $m$ and $n$):

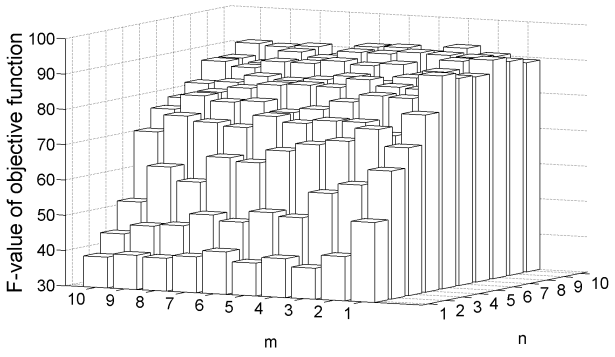


Fig. 2. Achievable Security Levels.

## VII. Discussion and Conclusion

In the present paper, we have taken up the generic model of [4] and specified it in order to apply it practically. The task of fuzzy decision models mainly lies in the operationalizing of the target function and their constraints concerning the linguistic expressions and their respective membership functions. As a proof of concept we have given necessary definitions and membership functions of the underlying fuzzy set theory and thus were able to operationalize the model. Due to the lack of exact solution methods in the area of linear fuzzy programming, we have developed a Monte Carlo heuristic.

As one can see in Figure 2, our analysis shows that there seems to be a linear relationship between the architecture $m$ and the security properties $n$. The overall security decreases with increasing $m$ whereas the overall security increases with the increase of $n$. The reason for this is the following. In order to reach a high security level in an OR connection, it is sufficient that one single involved component has a high security level which is in fact easier to realize at a high $n$ than at a low $n$. To get a high security level in an AND connection, for every $i = 1, \ldots, m$ the terms $\bigvee_{j=1}^{n_i} A_{ij}$ have to possess a high security level which is harder to realize at a high $m$ than at a low $m$. Both conjenctures have been statistically significant proven (see Table III) with a linear regression analysis which has a high quality of fit (Multiple $R^2 = 0.8197$): the estimated coefficient of $m$ shows a negative value ($\beta_1 = -0.9181$) whereas the estimated coefficient of $n$ is positive ($\beta_2 = 5.0966$).

For a deeper evaluation, and to use the model in praxis expediently, there are further investigations necessary in the form of case studies with enterprises from which one can derive budget restrictions, costs, security levels and structures of highly distributed systems. To operationalize the AND and OR operators, we have chosen the min and max operators based on the ranking from definition 5. Another option for this would be the use of intersection and union operators that are established in the fuzzy set literature (e.g., Yager, Hamacher or Dubois and Prade operators [23]). Plus, there might be further requirements defined for a distributed system parallely to the security, for instance, efficiency. This leads to a multi criteria decision problem. In addition to these provisions, we will develop other heuristics as well and evaluate them against each other. Finally, we will increase the architecture $m$ and the security properties $n$ to solve larger instances.

## Acknowledgment

The research leading to these results was supported by the "Bavarian State of Ministry, Education, Science and the Arts" as part of the FORSEC research association (https://www.bayforsec.de) and by the "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007-2013 (EFRE) as part of the SECBIT project (http://www.secbit.de).

## References

[1] R. Bojanc, B. Jerman-Blazic, and M. Tekavcic, "Managing the investment in information security technology by use of a quantitative modeling," *Information Processing and Management*, vol. 48, pp. 1031–1052, 2012.

[2] S. Distefano and A. Puliafito, "Achieving distributed system information security," in *Seventh International Conference on Computational Intelligence and Security, CIS*. IEEE, 2011, pp. 526 – 530.

[3] G. Sunye, E. Cunha de Almeida, Y. Le Traon, B. Baudry, and J.-M. Jezequel, "Model-based testing of global properties on large-scale distributed systems," *Information and Software Technology*, vol. 56, no. 7, p. 749762, 2014.

[4] G. Schryen, "A fuzzy model for it security investments," in *Sicherheit*, 2010, pp. 289–304.

[5] R. Böhme, "A comparison of market approaches to software vulnerability disclosure," in *Emerging Trends in Information and Communication Security*. Springer Berlin Heidelberg, 2006, pp. 298–311.

[6] L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Communications of the ACM*, vol. 46, no. 3, pp. 81–85, 2003.

[7] R. Bojanc and B. Jerman-Blazic, "Towards a standard approach for quantifying an ict security investment," *Computer Standards & Interfaces*, vol. 30, no. 4, pp. 216–222, 2008.

[8] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *First International Conference on Availability, Reliability and Security, ARES*. IEEE, 2006.

[9] H. Wei, D. Frinke, O. Carter, and C. Ritter, "Cost-benefit analysis for network intrusion detection systems," in *Proceedings of the 28th Annual Computer Security Conference*, 2001.

[10] U. Faisst, D. V. O. Prokein, and D. K. N. Wegmann, "Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmanahmen," *Zeitschrift für Betriebswirtschaft*, vol. 77, no. 5, pp. 511–538, 2007.

[11] L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM*, vol. 49, no. 1, pp. 121–125, 2006.

[12] V. C. Lee and L. Shao, "Estimating potential it security losses: An alternative quantitative approach," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 44–52, 2006.

[13] C. Huang, Q. Hu, and R. Behara, "Economics of information security investment in the case of simultaneous attacks," in *Workshop on the Economics of Information Security*, 2006.

[14] R. Böhme and T. Nowey, "Economic security metrics," in *DEPENDABILITY METRICS. LNCS 4909*. Springer Verlag, 2008, pp. 176–187.

[15] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.

[16] H. Cavusoglu, S. Raghunathan, and W. Yue, "Decision-theoretic and game-theoretic approaches to it security investment," *Journal of Management Information Systems*, vol. 25, no. 2, p. 281304, 2008.

[17] Y. Beresnevichiene, D. Pym, and S. Shiu, "Decision support for systems security investment," in *Network Operations and Management Symposium Workshops*. IEEE/IFIP, 2010, pp. 118–125.

[18] J. Wang, A. Chaudhury, and H. R. Rao, "Research note - a value-at-risk approach to information security investment," *Information Systems Research*, vol. 19, no. 1, pp. 106–120, 2008.

[19] E. Chew, M. Swanson, K. M. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance measurement guide for information security," NIST Special Publication 800-55 Revision 1, 2008.

[20] L. Khansa and D. Liginlal, "Quantifying the benefits of investing in information security," *Communications of the ACM*, vol. 52, no. 11, pp. 113–117, 2009.

[21] G. Tassey, M. P. Gallaher, A. O'Connor, and B. Kropp, "The economic impact of role-based access control," NIST Planning Report 02-1, Final Report, 2002.

[22] G. Schryen, "Is open source security a myth? What do vulnerability and patch data say," *Communications of the ACM*, vol. 54, no. 5, pp. 130–139, 2011.

[23] H.-J. Zimmermann, "Fuzzy set theory and its applications (4th ed.)," Norwell, MA, USA, 2001.

[24] M. Sugeno, "An introductory survey of fuzzy control," *Information Sciences*, vol. 36, p. 5983, 1985.

[25] C. Lee, "Fuzzy logic in control systems: fuzzy logic controller, parts i and ii," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 20, p. 404435, 1990.